From frank@funcom.com Tue Nov 9 13:24:21 1999
Date: Sat, 30 Oct 1999 20:40:25 +0200 (CEST)
From: Frank Andrew Stevenson <frank@funcom.com>
To: livid-dev@livid.on.openprojects.net
Subject: [Livid-dev] Working attack on DiskKey Hash

Through private communication with list readers, I was more or less challenged... (Or so it felt to me) To find an attack whereby the encrypted (temporary) diskkey can be retrieved from the hash found at the start of the Disk key data block.

At first it seemed to me that it required a workload of 2^40. And there didn't seem much in the way for speeding up such an attack. But through careful study of the structure in the mangling cipher and the CSS I have now come up with the following attack.

Guess the initals state of LFSR1, and B[0] - the first byte of the second stage of the mangling cipher. From this starting point k[0] and B[4] , first byte of mangling key, and fifth byte of second stage can be found. Now k[4] can be found, that is the fifth byte in the mangling key. Through a table all permissible k[1] second mangling keys can be found.

Since the mangling key is the output of the ordinary CSS cipher, LFSR1s output is completely known. We have also just found byte 1,2,5 of the CSS cipher output. This gives us 2 possibilities of 1,2,5 byte output from LFSR2. Luckily there is a 1 <-> 1 mapping of these bytes and the initial state.

So through a table with 2^24 entries the initial state of LSFR2 can be found. By now completing the mangle cipher 1 out 256 LFSR2 startstates will emerge as a candidate, and can be checked the usual (slow) way. There will 'only' be 2^17 such checks so performance is not a concern.

The whole attack has a complexity of 2^24 (mayby 25), with a memory requirnement of 64MB. On a PIII/450 it will recover a set of possible keys in less than in 20 seconds.

Sample run on 200MHz R4000 (?)

```
odin:~> time ./unhash fb 81 26 01 fe
CSS hash finder - gobbles memory ( 64 MB RAM ) Good luck

Searching for hash: fb 81 26 01 fe
Initializing k[1] lookup table
Initializing and clearing 64MB of RAM
Calculating big table. Wait, this takes time
--------------------------------
################################
Table init completed, now reversing hash

 Possible tmp key 21 5b 31 89 82
 Possible tmp key 3f 9d fa de f3
 Possible tmp key 53 4d fe 99 1e
114.602u 1.595s 1:59.12 97.5% 0+0k 0+0io 0pf+0w
```

This recovers 3 possible keys for the given hash.
I believe the wrong ones are easy to eliminate

by trying to decode the datastreams. (It takes
almost 2 minutes on this CPU, but at least it runs
on bigendians as well)

frank

--------- Fully functional DiskKey Hash cracker -----------

```
begin 640 unhash.c.Z
M'YV0(]*X&<.F#IDR('C,H4,FS1L7:'PH"#BPX,&$"^4(/`-1(D6"!A'R&$,G
M#YPR'2<*!'E1(4,V:<2D5+`P#)TT8T#4<3,GS1DW9<B`$$@'Q)`I4^B$$0-C
M2XP877KLJ<$"!HL8+&2PF,&"1M6K6;=V[;-#`4VE-W/N[/DS*(@Q:,+(,8I4
MJ9@86V34L!%5P1X%"6#@F<%5\(W"@\54Q2/#QF(;B&4@MJ'8L&/!,\HLOJS9
M\V7&E?'8Z,R8M(W/-Q0#%DP&<0[$9$+#^$P#,0S$-$+G^'QP<0[29#[#"$V#
M-`S2-#[G4!T83XT;BV-`%US#S&(<6@6/F8X'!_<QU@7'R.X\3'3SU,GC"()G
M#/KN[\>0CV%]-1XR.7SG9XU5,`RK@M&P'QXP#$A#?WCD`.!]./C6(&L+PH`@
M#0\26"$-"^:`E7TSD+&9AYA1)9@,7@EF`XB,H6B#B'C<4.)@8VP6(V8OZO78
MC(SA:,.+-U!E'QDHYH`B&2S"\"(-*,*`(@TLYO`B&3CF@",9+\+`(@TXPH`C
M#2_FX&-S-0P8PX`U((C#@F,,B,.`8R`8PX(U5!A#A34LB`."8U2(0X5C+/@4
M"S]REP-W9+`''WDT<`<#=S2PEP-Y9+R7PWMDD`<#>S2\!\-(-)"70WU@(A8#
M8C6$AL-G8R"&`V)CA!;#9S60%@-I>UT7VABDX4#:&)_%P)Q@8B!F!F)BA!;&
M9V4@%@9B981FQF=BD&8&:6)\MM1B99`6!FEE?&;&KX-Q=P-W,[`G`WDV<"<#
M=S:P=P-Y,[QWPWLSD"<#>S:\)\-(-I!W`ZC`#FC&@'<M%L:"90P8QH!E(&C&
M@F)4:S:%3!F,8!D5AE%A&0N:L2&8*,:`8@TLXO#B&"CB@.(8+,;P8@TXQH!C
M#2_BP.(8..*`XQ@OQO`EL"B:@:(8+(;Q8E`&HU@&BV:\*`:.9N`HQHMAL%@&
MCF'@6,:+9OP\V(`W###@#@C(L:,.`,@QH`X(W+#A#A3=4.,.",B!H0X4R5&C#
M@C=\#"QW9G`G!GMAD%<&=V%P5P9[9I`GQGMFO"<&>6&P5\9[8;Q7!GEFF*$`
M66;5E)9.//DSE%!PR4574DO)D-=>??W5W'^+25B[I;956:1PB@X(0X7#U:YI
MDED:JIE]XT4GJI]N]LJ=R]&U[.I[8T8G)WNS1A=RC/:1N)B-(WZV[O=TDVUO
M9"C*@..]WY.6]O=XA[8OH,W-\-D,Y+XX`XOU+D:8_VY#4+G\1YH.^0]',PA-
MO/PGM@;91T"+H5`$B<.I)6T)4\A9T(SBB"C<'.E*M(&.?4JUF!J\)TPEI!-[
M8E7"D<V,/#4@%9P05"OJ<(=F)?3:B6[T&'R91FUZ"TV^'O.B%3WF,^EZC-GL
MABZNV.=?FR'-#5!T`QRE9C/R`AO<4",N'K'H79M!3-LVX[<$><HU&4+0;GPC
MJ"XU23>2&E`.*O0IWY!&2+[A7G/.='TSJ4=5-2O99[QS'37IR53O4=EU<L8>
M7=S/6-`2G--8-+G%!,N2$$/0X"Q)K:%)+32/LR3!'-@<HQFL:-9"W(+"@*#"
M&4Q9*,J:P0BG+85ES%CF^5%H(K48_/2R0H7J)7"&-"5(P69!9$!0<'I)J"=Y
M+4V+R5,T;Q6?E>V,/;B*)IKP1)Y4I?-D-T.5")O3N<5,RYQ!@YJS("<PB7D+
M<:QC&N>SU;SR(DTP5\.6Y;C%L(V%YG+8.IK5D*4XA%W,<#/X7%G.8A.<D(XM
MIWM+7.9R%-8%:PMEDD'L[$.[$1U);4%R'&^<92BZ??0Q(;7D2,T),`*9-((@
M]8U(>TG2VKTT0#S5S*-42E.6/M*EWSNIB5(*R9X*IIS^N2D>(#A4F?*4-37E
MJ-**9*AJBXJ%:1L4#4H'J49BBU*E%A:I/I1I4KS95IS,5ZU%+6E:<?A6M3[U/
M5&<WU9R:,:ZQ\6E2V[I4N^XTK'(=*UWY2M4=PA6P>5VK30GKU[0&5K%D[:I;
MSWI7Q-9TKY+MZULK>]650G:PF2VL5;&J5JVR-;2-Q>M<,<L8H585K)W-ZE8[
MVEJSOO:PL2UM.2-;V\G>EK.D?:QI%XO:S?XUM\+=+6A[JUG*'C>XB1TN:[WG
M6\,"U[/#Y2UUF_O;YV)WMG4UKF.CJ]SINM:ZWI7M:9DK6MA"=[5<96]J+:O7
M^&ZWO;A]KV#-:UOTCO>R]CWO:+_;4MK>=[[()>]Z#RQ>U>XWP/T=L'J)*]\&
MT_>S_*VNA'6[8`&[E\`_-;"'\POB#'/7OP[&,(0U_.S)FQB_UYVP=D<<8PY3
MF,'._>^#11SA%MOXQ0C6KXIY%&(2NWC%)]YP<@L<WARG6+I(AG%Z;3SC'AOY
MQUS.,HBK7.0:+_G&-)[RE[F<9!]_&<@63C'\B5SF*Y\YRVD6<G:7B^/NZEBQ
M:';RA>><9SL_&;R,C?.6Z1SF.T.9S5(V=.<4&CJT.'0MIG-+ZBA:EZ70X'5\
MZ8%?>,O''*&);JLT&\+\E"SX(=-MS.-;QZS"43U=B$]XRYC>-B8G.M()F'*C
M&-PD1DK_U.Q()ZL1U8IXM)YUZ65/TI_3>,0UKW`T9UO:V?JPIB.MQ2Q*,YL2
M`J5F1:CIT3_JO50W[44Y=!EN/IZ"(:3@Y3A_<4XK'STDI^*C+\SQ2W/4D]0)
M*44OR<D+<KF<W2!I@RKQ6ON)R.J5<F#%F_M!"S7><@Q'<X6<7;E/6Z;AEJSN
M2"O@%)!:4I36\69GI@GAB6RMM-O%W*1&&BI3@)IDF\/*6*!"VA::(U*8VA@F
M)CF2:4"^Q`S'P";P_'"T9%>Z&8O`AX>J/<9J+6L2BTC62_Y1\HM,\YJ2KK.D
ME:4OEBI26LB"-+(AH<B`0/L0.D.L*MRP*C+*F@RS1.4:4LS&,?\#EAB%Y<39
MF8HXMY*?L83X3U?I)COD+&T"-1F:*QX57(NZ#J.^HR[$L4MQSQ/4#0E%+L&)
M"W#C]$\C,85-<Q$.7Y;#GJ-6R)Y@8H8]FSO,XSP'.K/8X0UI$$I%;T('-I1A
M#67'0PQ0`.FVH&ZB(%'!\//`@N)'=-+)3T,;4K#I'#C?+40!`1VP0@>MT($K
M=/`*':A"!QN4Q?JE,[YS5;<&C';A_-E/PT(3L/T>2'\+,.@"'\3SG_-WW_YM
MX!3O!QC?!X!YT04@P`<@@`+W-P-=P`,\@`,ID(`+>'\T\(`\\"HIX`\TT_/?
```

```
M9P(WX'\SX($SH`(RL`(XT`+AYW\UT`,P<'YF\`9RP(`NN`-IP`,U8(,KL`+4
MEP"ROW\=N'NMLP7=UP5>((07M7T#F`#T)P,>&`,^X`,Q<'[T8P,]@`(HL'TF
M$`,I`($2Z`4K"!A`V`-(>&GAMX3T9P-7B(5LF(4S$(4SD`)@&(=1R(5SF`)1
M^(7?AX<^4`,I8`)K184%Z(9>F`)\4'Z"J(9E2(1\(8@UL`(>:`,K$(9,V'YI
M$!7C!XBFY8A1V`,X<'Y]`!@Q.(-IT`,Y8(,^4(-IT`(MT(,)L'Q;@(1-D08K
M`!51T7ZRN`6T:(M'6&EWL06PF(N[V`7$Z`7!Z(NS2(QE$8IF\0(J\(S0&(W2
M.(W46(W6>(TJH`#)IXTJ``(@0`5H@!`5!0)($`9S@`8@(`=E8`=E(`=S$`9L
MP(W<Z(U$L(YI,`=N$09N(!1WH!8T0`=EX`8@(`9Y``)&(`?ZN`8@$`0N``))
ML8X!.0=OX`;RF'S>B`(@8`8(Z09K``1FL!-C\`9MX`(AV08@0'T6"0)24`:^
M9XYN,9$@$`8@<`10P`0@`!.XPA-E4)'8V),^^9/3^`)F,0('808"@1!+$`-4
M$`1"P`1%<`5)0`14@`0@\";-V(T]T09PX'L9"9(W`9-T\`9O,9'L*`=%$8YX
M,)!Y`)!SH'UBF7TJ()3."`)N\`8`J0,@<`=IP`9L``)GD`;LF([Z2`8BF8YE
M,`=UP`9TT)9I8`9T.9%H"0(-\9>+&9/J.!1N``=U4!1QV6@-E1/0AY:3F0:+
MZ10W@(`]``(B("&2P23ILB9+@3*+PP4P(`(+)3H.E7U(4`9X(`1K6094\`9)
MX`9T@)$AR1-%`7TJ``=.4`=MS"US,8%_X8WO!Q=EX8W9)P<+19WHF)IAR09O
M<`?MB)',Z9S0B7\(N(':F(X@D)JO8I$,2)PI@)$9`1<S"``*BZ1.D.0<L(%$G
M"0(M@)^\.9J5J9[<V9YN"9[B>9_E^9SM*(`G>9WI"(D5*)_T20=R8)\8F9^4
MR9_^.8$!RJ'[&:%FX8WJ2`=U(`<".1<F``*B9P8[X(US*1!V`(^YAYF:611Z
MR9?X&0:!"0=R\`9D4`>XXI=R\3AG@!"=V0<@8!97.8]3('U;B1`?.1!?*9!A
MJ7V'612-&9-O,9BY9Q,(L7P@`*1"2J2'J7WAZ)>`&9`]>H[<*)0*<'LW2J-;
MZA-BBI'7=WQRT8UQ<8[]N:?K-Q?*]Y_3^5"1QJ=S(7VNTXCK*:C0!P>PZ*CK_
MV09ET`9C``=Y@)&,VI]_B@;]60,DBIUMX#HU@)HN*J&6BJF:2I[+UY)K$*JC
M6J:P>*H(^H*`L7NDZ7O+-WQ#4:K]*:G!1Z+KV9@8N:ICH)6<"JRT&GRR.H$]
MD)HP8*CKZ8UEJA'$:088*0(@``5O,`<](09<20=:"0)D6@*'DI;H*@/JFJX@
ML*[MRJY<X`8B`*OH::]08:\:9:\.:*\7.*O,R(Q7"0)-$`8"T956ZA`"V9G9
MUP8&ZP:<2IR6>08Q,JC=*!=G8`=;D)X@@<*B0BGQ!X'X(N@<N^A4`4A4@0!8@
M,)>?ZA8-,0<*2:8!NA,YZI8@X+!N<`9<.09I``?A2*A"Z8T?JSI"(+*I2;(G
MF[0I&Z-S.057,Y8"P3I)"@)OX)@XJ[,(P;,^VX[)%[2(JG[0-P1&V[$EF[0H
MJ[)S^02;6;-2BQ!5>[/ZB+5C7;,_"Z`@,)P`*0>6VA!BN@3#&I=-*K3I]WS(
MUWZV>K1E:[)GR[3=6+`Y"Q,Y.[=;.Q<RNY!L()%4N[:;F9%!:I(5A9%#\)^=
M*;@0)6G(]P:,B1>G&J/6VKJNN[+=:)2!:93N6!2H2P<U2Y!L2;6.R01&,`52
MS`-=^ZB#:[JJ<[NF^GZON[RPFY%MZKRUF[FXN[FZFZ9OZ[O`*P/#2[J)BIE%
MP09F,`=RS`-AP+K,^[IS60=P<!)SD0,#.:+7^[O!N[U?&U'9![[BZROF>[ZM
M.Y<*RK4X\+Z5&;_`*[RC6[_8)['D"@?]N<!:H7U:R140#`?BIY4Y6*P2FP8L
MH`82*JC9YP8/"0=!L+_]VXVDV8XV(8,9J<+8.[\U898@(#I*ZK4>++$@#)!P
M(`0D;*TSFK<I/!>C6*;?&JY<6;3YY[H'7,-%X094(`=YL,,E/!0^')9`K,)+
M`*%P,,0QL9>DF09IFL3%*Q0?[*W@&A.^EY3F.Y<C\+997,;BBI006J,%\<4T
M',86"P)):1>^1\)SR01O\`9KH+[:MQ1<&<1M3,1P#!7TJ\3="`)"X!-40,AE
ML+]]++_:^\*+B18((1`'@0=N09!5&1:B>KNY^YO#NYYS>03J6`8W$;D'#*1$
MH:VJ.8Z?ZKS[R+4!>@9O4"R^UY:K*H,%B9S[0K!"H))!T`3_>01_+!0%,09K
M,*_SRJWJB<K=.`3AZ,P3ZYP!69D*;*P3FQ,@$`*I:0/4VKJPG*W;6@7OF*1X
M60)MB0=I"<\@(,_TG)8868[GZ!9S<(\Q.ZPIS,W]B;$:>\0&:JTGFJ("V0)3
MN)[,**/53);MR*69N;D8J\W$V9996LL'/(J<>JLQF@8)`0*B^M$[6,[6&K)#
M`0*HNIN]^9O!B;<8*="Z6(OI*:&AZ(WG3`>R+`).*Q=PL1$K/!>?VL[N"J_O
M6M1(+:_TVI\AFW],+8!/O:\+N07].M7_.LT.7:W="`7J"`=R@1!ZG*9!7,OJ
M6);O&(_6VIG4C)E=;*-Z@!#@"<B"'-9M&<3MI\BOC*TZO:W#V=8PH0=`?=<(
M&->!#`>#_,;17-!Y+,D(ZK!\^09C(,PD8S\6F91+V91/&953.:NKBH_%B<<Q
MS-;].:W]N2(Q1,[=:-E,Z910*9546=#>O-AOW)ZIZ015P`0V*9W5>JVQO*UJ
M:[M6>ZG`#`+M&*1RT)^1T@8"FO>H&\-H@+IL(!3XB!!W$!=%D01YN9=]Z=C@
MF1-`@0=%H0.M&,VSZHV\29H8J=``NYX+C*!-C8!>L#IV@1=3K<@#Z(T<G=+2
M"@(?'=)Z0<XDO0+_.9>"W;7>>*C>Z,`(BH3TW={Q#=+*.Y<,O@6.#*%=<,#X
M+8,8J0:WRM\@P.$\``+_[>%J4-(3.)=&C("`B^#6NL`S@*`<'M\*_N",:Q00
MBN$MKI4T@*"R[7L4KMJ8W=J;W8T8.>+=R.$"[N+_&>'=&)([`=S$39P:D:8_
M.\.[G>`ZOH,2VKK>O,`['JV@?=FLK=FOW;%7;JTYO=.1/-LO:XYY^ZYD`-`3
MO.,%W;HW[;I=KN,A#>1C[MK_V>-E\.-*N=J9[>=$+N)[89%(/L$O/H%)KN>H
M*G]G#NB"+N:%/N0+B.BH_>$@\.APT.@JC:!>ON4IR]`EVKQ]W<IGD+ESL9+P
MR`8%*08^<=A<F=>]K9JIG@9N%=2#^18MB:VKOB--4,QO*P7'G-@2^LAGL.9<
MF9K<#=D8^2KC\B[OB95I\-95&Y]T,($%W=FLC)'*SNR:X:(@T)_2/BYUL^D]
M@>W:2A3<+J&Q'=J,#>:VC=LFC=-ZO=._S;LW*]Q.3-QR8-P-&02,Z9AT@`;W
MF)?0309N<`)GF:)T0-YU3MQX@-X`*KP%?>=*+JT2FN;;.@3P.`:)V5"1*^NK
M'M8-%04&2P<-C/`8'0;`A]'25P;(OIX>KYJLF/,ZO_,\W_,[+_$2FM\@O=_]
M'>+G3NT`/A0F;N9<+LL,"`(MZA__TCEF`*W[K=NO>_,B,`+23.KX;08%<8X7
M2IB;._%WCN6&G9I8F-("#M(3&/5X0!]4_S#_J8""$<`*V-%P?P/E'=0;WN$Q
```

```
M"N(B3>)+_X-H[X1MR(83#(<G"89:R8=VN,!\J(>/'X5^J(F=0X5HWYY9J)6$
M>(A:*0.:+[VNHP:HNH@3K+WW;:UGS^EJ3_KHF1!&3\X3F/>PK\@0"`(!7/NP
M?X&D'NZ2O`6FCZ"2[HUWKO5`[Z19G=8@<`4(\=62.9&;[`9=G+/]69=W8)AF
MC1"?JM5>J_7BSM;)*9)3"I`>\IC97];MV!.1^ZG03*^SNL"BFIKO#0+Q/>'U
MC8"KG]\W7`8B#/AT*80$@9!FVBA;C.I__Z_P[3;\-;YDDK2*>_^!`F$D!#@`
MHY#NZWL,T$<@*`H(]5S4)CIU#FTF!204!I`&'^U:"-*KE.TNC528,B#]RG#W
M:>B1NZ(W^`+<O<MQ:4^^#:&;$+[&EQ@(=??/$\T`"I<!9=+J:UT9\`>FIB((
M`BS@0GM=3$#MH8`BN(6Z4`2:0#).*WD]Z47?(-R"\T679H*I-$+7T'A8DW-.
M.>KY[:,O!1<0@D2R5""@1FDS2=:6<)S8.F*IB0-:P$^TV\26(LN#`K`#!J+=
MUM[H'U6#;SKP$UDU_4?J$$QJPG_U;P#MMJ9U.3(4.CIX0:H.G`$T].JSF!LK
M8K$/Q_&_$$;,B$X`Q&'$+,2-N`-("A4@^NI&ZL\=(02O9I;:TMLZ>`CA:D&N
M5:>UZA:.\T8I;@.2PBW8?O!@(J1OP1`1WD'E=>:*UK]*3<$POA5#1.C`B.$6
MHW]WNV(2CSID9@PAR+$Z(-946('[A7Z/+C6Q@F0*F=B_"W'>4(N]L7!X``>B
M*UQ>!2XU4;HP9P[)''Q2A\&P'0H@1R<0_YV`$UY'T'45K3\XP425-!1`VVEY
MS25U=)PR`I&R79JK*+!`D]3"M!=`1'LO[O7QGVDEX*:AW;I=>(&@;4$OA+QB
MGW>*8(+P`S*OC<?HDN*;F$8_P`,^11"`EP;A4D2*KT_)]40($:"`(H2:>*VK
M*))$)0?W,M^9PXD("B/MQ$YGKJXA`NJ*J<LM]KVPN)E<!S8DBQXP\X5`D">0
MHD55XEV.Z90QK[G$EF1B&HA>^'"V$<5_=1/G7$J$?4<L][TGWH>1Q"("RGV[
MCP(MQI#8NKP<@@)^Y-`Q<D9K);8TBJC3<V411IU$&^>``J-GW(/_*34.11N'
M#3'2:_0!58GV)46SR+R*5FM\A+X(&<I$1-A^M"$M'(W>J/W\QJEF&H.@1:$O
M(:LU(D+?B!PKG&DSCL^1PE$''(-@66^/].X2SL?U<Q_QG_XXAA0M9IG$Z'J#9
MZ,W``81RCO--.QX@[MA^1$RH^T]@3FS91XYEIQ8"G@)(&,D$U+_^9`*6883B
M7R#0=<TE*K"E8MC36H.)D2MMQA?HNB;DZYN0`FZMQ,:\J!JO(@5[C$4Q,LZ^
MNI?I+*/LNX"\;S/.1L\(#2$9\!.-L[$THBK/*!M7H]A:CK91S\'&M\<A8Z1<
MS(HZ$C=.QMW8(9?7=L2.\3$;ZK_R6!R5H5L,CX?OO<U'^+@4H&.45(\.:#86
MK?&(_[8C<8R2WS$+KD;QB*I"EB"CDHH0/2()^+8EJV-[K'!GTCQ:QS79$O>C
M-()Z-LY.3J#^>!/.0)Z">@,2ZAG(#80@SUP9-'ZGK@QJI&R!D0#=K$J490#<
1N<C9AM4,$XI246J11`DLLP`2
`
end
```

This sentence is unique in this respect; it can safely
be attributed to my employer, Funcom Oslo AS.
E3D2BCADBEF8C82F A5891D2B6730EA1B PGPmail preferred, finger for key
There is no place like N59 50.558' E010 50.870'. (WGS84)